1. Does the Government intend to impose the provisions of FAR clause 52.222-41? Service Contract Act, as amended?

ANSWER: The FAR clause 52.222-41 is not in the solicitation; therefore, it is not applicable to the solicitation or resultant contract.

2. Ref. the CLIN x006, Customer Service Incentive, on Schedule B – This amount is based on results that are unknown at this time. For proposal purposes, what do offerors put on this line? Should CLIN x006 be preprinted with the same figure for all offerors?

ANSWER: Contract line item number x006, Customer Service Incentive is, at this time, for administrative purposes only. Offerors are not to price this line item.

3. In an effort to reduce costs of this program, HMHS assumes that the Government will allow the contractor the authority to commingle Government furnished supplies as referenced by the FAR Part 45.507(e) as flowed down through 52.245-2 Government Property (Fixed Price Contracts) referenced in Section I of the RFP. Is this correct?

ANSWER: The requirements for tracking pharmaceuticals received from the Prime Vendor are referenced in the RFP and the Government property clauses referenced in Section I. Commingling is not objectionable, however, the contractor must abide by the inventory tracking requirements referenced in the RFP and embodied in the referenced Government property clause.

4. Would the Government please provide the following data:

a. The number of unique NMOP users for 4th QTR FY01 and 1st QTR FY02
b. The number of NMOP prescription orders received for 4th QTR FY01 and 1st QTR FY02
c. The number of NMOP prescriptions filled for 4th QTR FY01 and 1st QTR FY02

ANSWER:

Month	Unique Users	Rx Orders	Rx Filled
July 01	122,907	Not available	283,514
August 01	123,235	Not available	272,199
September 01	123,603	Not available	281,392
October 01	146,058	Not available	343,782
November 01	137,780	Not available	309,404
December 01	148,373	Not available	347,060
January 02	165,074	Not available	390,002
4th Qtr FY 01	237,899	Not available	837,105
1st Qtr FY 02	272,534	Not available	970,240

5. Is Option Period 5 really 8 months? If yes, then the number of prescriptions (6,734,860) seems to be overstated.

ANSWER: Yes, Option Period 5 is an 8 month performance period. The number of estimated prescriptions in Schedule B should be 4,512,356. This number will be revised in an upcoming amendment.

6. Ref. Section L.12.b - does the Government want offerors to submit two paper copies of the technical proposal, past performance

information, and the cost proposal along with the CD-ROMs that are required?

ANSWER: Paragraph L.12.b. states to submit the following in electronic media as indicated:

(1) CD-ROM in Microsoft Office 97 Word
Two of the written portion of the technical proposal
Two of the past performance information
(2) CD-ROM in Microsoft Office 97 Excel
(3) Two of the cost proposal

Clarification of this instruction – submit two CD-ROMs that contain the written portion of the technical proposal; submit another two CD-ROMs containing past performance information; and submit two CD-ROMs containing the cost proposal.

7. On Standard Form 33 (top page of the solicitation), box 15a, please define "code" and "facility" boxes. Where can these references be found?

ANSWER: Offerors are not required to fill in the code or facility in block 15A.

8. On Standard Form 33 (top page of the solicitation), box 15c, states enter address in "Schedule". To which schedule does this refer?

ANSWER: The "Schedule" referred to is Section B, Supplies or Services and Prices/Costs. If remittance address is different from address put in block 15A, put remittance address at the end of the contract line items in Section B.

9. With regard to the estimated prescription quantities outlined in the "Supplies or Services and Prices/Costs" section, what confidence rate does the DoD assign to the figures? Will the DoD allow for pricing adjustments if estimated quantities are not met?

ANSWER: The Government has taken reasonable care in the development of the estimated quantities. Estimated quantities are based on historical data and escalated for option periods in accordance with observed pharmaceutical utilization trends. As a result, we do not anticipate the need for any subsequent price adjustment(s).

10. C.3. With regard to initial inventory, will the DoD purchase the inventory from the PV and supply it to the contractor? With regard to replenishment, will the DoD reimburse the PV without invoicing the contractor? Will the DoD or the contractor be considered the owner of the inventory? Can you please explain the inventory reconciliation process in detail?

ANSWER: The TMOP contractor shall dispense pharmaceuticals from its on-hand inventory and replenish dispensed pharmaceuticals through the Prime Vendor. The TMOP contractor will order replenishment pharmaceuticals from the Prime Vendor and take receipt of the pharmaceuticals on behalf of the Government. The Government will directly reimburse the Prime Vendor for the pharmaceuticals accepted by the TMOP contractor. DoD will be the owner of any inventory in excess of replenishment quantities until the excess is dispensed. These quantities will be reported in accordance with Section F.4.

The reconciliation process relates to reconciling pharmaceuticals ordered, dispensed and lost for any reason. The frequency of ordering is at the discretion of the TMOP contractor.

11. C.4.2.3. In the event the contractor receives an insufficient co-pay from a beneficiary, the contractor is required to fill the prescription and bill the beneficiary for the difference. How long is the contractor required to carry the Account Receivable and can the contractor bill the DoD if payment is not submitted?

ANSWER: The contractor shall follow its normal business practice for collecting insufficient or delinquent co-pays. The contractor shall continue to fill prescriptions for beneficiaries delinquent in submitting co-pay amounts until the delinquent balance equals or exceeds $100.00. The DoD will not pay the outstanding balance on beneficiaries' accounts due to partial or uncollected co-pays.

12. C.4.2.3. With regard to three-tier benefits when is the expected effective date of the benefit change from two-tier to three-tier?

ANSWER: We project that the three-tier co-payment structure will be effective in the first quarter of FY 03.

13. C.4.6 Will the DoD produce and provide a name and address file so the contractor may complete the beneficiary mailing?

ANSWER: Yes.

14. C.4.8. Please provide complete definition of "personnel dedicated"?

ANSWER: "Personnel dedicated" means that these employees will work only on functions related to performance of the TMOP contract.

15. C.4.8.4. With regard to web site information, will the DoD provide an eligibility file to the contractor which will allow the beneficiary to access their personal information, or is it a requirement for the web site to directly reference DEERS enrollment status to perform the functions outlined in this section.

ANSWER: There is no requirement for the web site to link to DEERS. When a beneficiary submits a refill order, it will be the responsibility of the contractor to verify eligibility through PDTS before dispensing the prescription.

16. C 4.9.2. With regard to the open refill file, will the DoD provide the file format at the time of contract award?

ANSWER: No. Appropriate file format will be worked out with the outgoing contractor. The outgoing contractor will have the file available to transfer three working days after expiration of its contract if allowed by state law where the incoming contractor resides.

17. H.1. With regard to clinical change orders, will the DoD allow for an "equitable adjustment" for pricing? Is the Government interested immediately in opportunities to improve clinical management of drug therapy? Would the Government entertain such proposals in the initial proposal submission?

ANSWER: Whenever the Government issues a change order, the contractor has the option of requesting an equitable adjustment. The Government does not desire any proposal information beyond what is specified in the RFP.

18. K.12.52.219-1(a)(1) Please provide the NAICS code.

ANSWER: The NAICS code is 446110. The small business size standard is $6,000,000.00.

19. L.8. 52.215-20 REQUIREMENTS FOR COST OR PRICING DATA OR INFORMATION OTHER THAN COST OR PRICING DATA (OCT 1997), paragraph (a). With regard to cost and pricing data, we assume this contact is competitively awarded and therefore is exempt from the requirement to submit cost or pricing data. Is our assumption accurate?

ANSWER: It is anticipated the award will be based on adequate price competition and not require cost or pricing data. However, in the event it is determined cost or pricing data or information other than cost or pricing data is needed to determine price reasonableness offerors may be required to submit such data.

20. C.4.3. What is a full definition/description of TRICARE Encounter Data? Is the TED the main form of data transmission into the PDTS? Is TED the replacement for the HCSR (Health Care Service Record) and, if so, has TED replaced HCSR worldwide at this point? Can TED transaction format documentation be provided at this time? (required fields, record format). Is the TED record intended to be transmitted concurrent with NCPDP v5.1 DUR transactions to PDTS? In other words, should the contractor expect to send two separate records to PDTS with each claim adjudicated (TED and NCPDP v5.1 as two separate records), or is the TED record a subset of the NCPDP v5.1 claim transaction format (in which case one record be transmitted to transmit both the TED and NCPDP v5.1 DUR verification requirements)?

ANSWER: Full information regarding TED records may be obtained from the TRICARE Systems Manual. The TSM can be accessed via the web at the address listed in Section J, Attachment 3 to Section C. Data to support the TED will be drawn from PDTS. TED does not require data beyond what will be required by PDTS. Only one transaction in NCPDP 5.1 format to PDTS will be required.

21. C.4.6. At the T-NEX Industry forum and again at the national TRICARE Conference in February, the Department has indicated procuring national marketing services as a single, nation-wide contract to cover the TRICARE program across all regional contractors. Will the awardee of the TMOP have any interface with that national contractor? Will the TMOP marketing duties be transferred to the national contractor when that contract is procured and awarded?

ANSWER: Marketing for TMOP will be the responsibility of the TMOP contractor. If coordination with the national marketing contractor is necessary at some point, the contractor shall contact the Contracting Officer for guidance.

22. C.4.6. With regard to marketing information, please provide:

a. an estimate of the initial quantity to be mailed
b. an estimate of ongoing mailings expected in each contract year
c. an estimate of the annual supply required to supply the MTF's,

TRICARE Service Centers and other representatives of the Military Health System.

ANSWER: The RFP provides information relevant to determining the appropriate quantity of initial marketing mailings. The RFP requires that the offeror develop and propose a marketing strategy that the Government will evaluate as part of the source selection. Volume and frequency of additional mailings will be based on that strategy. There will be a requirement to supply marketing materials to the MTFs, TSCs, and other representatives of the MHS. This requirement will be included in a forthcoming amendment to the solicitation. The current NMOP contractor distributed approximately 500,000 copies of their marketing brochure to MTFs, TRICARE Service Centers and other MHS locations in CY 01.

23. C.4.9. Contract performance is required 120 days after award. What are the responsibilities and the time requirements of the outgoing contractor to provide pertinent information to the awarded contractor?

ANSWER: We are establishing a Memorandum of Agreement with the outgoing contractor which should support the requirements levied on the incoming contractor specified in Section C.4.9.

24. L.12.e. When does the Government expect to issue a regulation and then implement its uniform formulary?

ANSWER: Publication of the proposed Uniform Formulary Rule is projected to occur by the end of April 2002. Implementation is contingent upon publication of the Final Rule, which we estimate will occur in 1st Quarter FY 03.

25. L.13.b. How soon after proposal submission does the Government expect to schedule oral presentations?

ANSWER: We anticipate beginning oral presentations within 7-10 days after receipt of proposals.

26. C.3.3. makes reference to an attachment (ICD, attachment 5, Section J). The attachment was not included in the solicitation.

ANSWER: The link to the Interface Control Document is available on the web at http://www.pec.ha.osd.mil. Websites are listed at Section J, Attachment 3 to Section C.

27. L.12. With regard to submission of the oral presentation we are directed to send the oral presentation graphics with the Technical proposal, but are required to submit the technical proposal on a CD-ROM in Microsoft Word. Are the oral presentation graphics to be in Word or are we permitted to use PowerPoint, or if not, in Word, can we only submit paper copies?

ANSWER: The oral presentation graphics may be submitted in either Word or Power Point.

28. L.12. With regard to proposal submission, is the prospective offeror required to return a signed copy of the entire MDA906-02-R-0002 with the technical proposal?

ANSWER: Prospective offerors are to submit the following as part of their proposal:

a. A completed and signed Standard Form 33 (fill in the portion labeled **OFFER (Must be fully completed by offeror)**
b. Fill-in Section B, Supplies or Services and Prices/Costs
c. Complete Section K, Representations, Certifications and Other Statement of Offerors and submit the entire section with the proposal.

29. L.11.f. With regard to the 120 day proposal acceptance period; is it necessary to state the 120 period elsewhere other than on the Form 33 (cover sheet)?

ANSWER: No.

30. C.4.1. states "The contractor will service beneficiaries with OHI when split billing and coordination of benefits is available through NCPDP transactions. The OHI will be the first payor". Will the selected contractor be required to support any level of COB process upon implementation of Option Period I in 2002? If so, what COB requirements must be supported?

ANSWER: Until split billing is available through NCPDP transaction, OHI will be queried via PDTS prior to dispensing the prescription and the prescription shall be dispensed in accordance with Section C.4.

31. C.4.2.5. states "The contractor shall not be required to recoup the cost of dispensed prescriptions if they are based on an inaccurate DEERS eligibility response". Does this mean that the selected contractor can expect not to be subject to retrospective payment adjustments (retro-actively applied withholds/chargebacks) applied by TMA or a TMA-assigned entity as a result of DEERS data inaccuracies?

ANSWER: That is correct. If a prescription is dispensed based on an erroneous DEERS eligibility response, the contractor will be paid the administrative fee upon acceptance of the TED. TMA will perform recoupment functions from the beneficiary as necessary.

32. C.4.5.3. outlines requirements for the contractor to ensure compliance with DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Can TMA provide contractors with documentation of requirements for DITSCAP Certification and Accreditation at this point (during the RFP response period in March)?

ANSWER: DODI 5200.40 is available on the web at http://www.dtic.mil/whs/directives/corres/ins1.html

For Personnel Security, Appendix K to DOD 5200.2-R is attached in draft form at the end of this question set. We believe the draft to be in final form and anticipate final approval shortly.

33. F.2. outlines the periods of performance, referencing Option Period II, III, IV, and V. Are there differences in contract-required services or service levels associated with these different Option Periods? If so, what are the differences?

ANSWER: No. The option periods simply denote future years for contract performance.

34. H.2. With regard to Financial Incentives for Customer Service, to what specific time periods of the contract do the incentives apply?

ANSWER: Customer service will be measured on a quarterly basis with the results provided to the contractor 60 calendar days following the end of the quarter. The quarterly incentive amount listed in Section H.2 is the maximum that may be earned in any quarter.

35. L.13.b.(2). With regard to the oral presentations; is there a maximum number of participants that the prospective vendor may bring?

ANSWER: Oral presentations are to be conducted by the individual responsible for a given element. We would prefer to keep the number of participants to a small number, but we have not limited the number of participants an offeror may bring. As stated in the RFP, consultants are not allowed.

36. If the Prime Vendor's shipment is delayed affecting prescription turnaround time, will the contractor be held accountable as part of the performance standards? How should this situation be handled?

ANSWER: We believe the prescription turnaround standard is sufficiently broad so that most delays will not pose a problem. However, in extraordinary situations, the Contracting Officer will consider the relevant facts and take appropriate action.

37. Are there any additional requirements of the contractor to validate the receipt of goods from the Prime Vendor beyond the reporting requirements identified in Section F.4(f)? How will deliveries to the contractor be reconciled among the contractor, TMA and the Prime Vendor?

ANSWER: When the truck arrives at the TMOP warehouse with the TMOP order, the TMOP will be responsible for receiving the material (physical count and inspection) the same way as they handle their commercial business. They will only sign off on what is received, not what they ordered or what's on the packing slip. The TMOP and Prime Vendor will work out any short shipments, mispicks or latent defects. DSCP will assist is resolving any disagreements between the Prime Vendor and the TMOP contractor, or manufacturers.

38. Will TMA consider the use of best commercial practice for its 6-month pharmaceutical dating requirement (as referenced in National Prime Vendor Solicitation No. SP0200-02-R-0001 Section 8(b)) in order to maximize inventory management efficiency?

ANSWER: Inventory management may be conducted according to the offeror's normal business practice and in compliance with the Government furnished property requirements of this RFP.

39. How will information be communicated among the selected Prime Vendor, DSCP and TMA regarding issues which may affect contractor's performance? When and how will the contractor be notified of issues affecting service delivery (e.g., back-order information, delivery status)? Can the contractor be included on applicable reports generated?

ANSWER: Communications will be through the Contracting Officer or designated representative.

40. What procedural and/or financial remedies exist for the contractor if it is demonstrated and proven that the contractor's inability to perform is caused by actions of the Prime Vendor?

ANSWER: The TMOP contract does not provide the contractor with affirmative remedies in the event that the Prime Vendor fails to deliver as required by its contract with DSCP. The Government will not hold the TMOP contractor accountable if the Prime Vendor's failure to deliver ordered pharmaceuticals in accordance with its contract affects the TMOP contractor's ability to meet the performance standards specified in Section C of the RFP. If the failure of the Prime Vendor to deliver as required significantly impacts the ability of the TMOP contractor to perform at all, the contractor shall notify the Contracting Officer.

41. Will the Prime Vendor stock all available products that are the most economical to the Government under the Federal Supply Schedule?

ANSWER: No. The Prime Vendor is required obtain and to have required products delivered to the TMOP contractor within seven calendar days of receipt of the order for products that are most economical to the Government based on federal pricing.

42. How quickly will the Managed Care Pricing File change upon selection of a new generic product? How will runout of existing generic products be priced, particularly if it is a higher price than the new generic product?

ANSWER: Monthly or bi-weekly as a normal Standard Operating Procedure. In the event of a breakthrough medication or a large pricing saving, DSCP will fax MCPF amendments to both the TMOP contractor and Prime Vendor. Runout product will be priced at the acquisition cost of the product actually dispensed.

43. How quickly will the contractor be required to obtain and dispense newly selected generic products?

ANSWER: The contractor will generally be required to provide newly selected (e.g., newly FDA approved, new contract award, etc.) generic products within 30 calendar days.

44. Will the Prime Vendor utilize drop shipments for processing orders?

ANSWER: Yes, in those cases where the manufacturers demand drop shipment for specific products.

45. In the event of mid-month patent expiration, when will the appropriate changes to the Managed Care Pricing File maintained on PDTS be made?
ANSWER: Changes will be made as stated in #42 above.

46. How will the contractor and Prime Vendor be notified of adds, changes and deletes to the Managed Care Pricing File?

ANSWER: Notification will be through the Contracting Officer or designated representative.

47. Will the contractor be able to access an electronic copy of the Managed Care Pricing File through PDTS, DSCP or TMA for internal review, auditing and analysis?

ANSWER: DSCP will make the MCPF available to the TMOP contractor on a secure server to download a soft copy.

48. What considerations does PEC, TMA and DSCP make when balancing patient safety concerns regarding use of multiple generic products with financial savings to the Government using Federal Supply Schedule drugs and pricing? Is there any limit regarding how often a manufacturer can change on a particular product?

ANSWER: Currently, the Government does not anticipate switching between generic drugs any more frequently than annually. The solicitation will be amended to clarify under what circumstances and according to what limitations the TMOP contractor will be expected to change from one generic manufacturer to another.

49. Please further define TMA's definition of "spoilage" as presented in the Reconciliation Report in Section F.4(f). Does "spoilage" include recalled, expired, damaged or any other type of product?

ANSWER: This requirement has been deleted and will be updated in an amendment to the solicitation.

50. Please further define TMA's definition of "product returned to the Government" as presented in the Reconciliation Report in Section F.4(f). Does "product returned to the Government" include returns to the Prime Vendor due to shipping errors, expired, damaged or products returned directly to the Government or another agent of the Government?

ANSWER: This requirement has been deleted and will be updated in an amendment to the solicitation.

PROPOSED
DRAFT APPENDIX K

INFORMATION TECHNOLOGY (IT) POSITIONS

1. PURPOSE

This appendix establishes standard designations for positions that allow individuals to directly or indirectly affect the operation of unclassified information technology (IT) resources and systems processing unclassified, For Official Use Only (FOUO), and other sensitive information. Such positions are referred to as IT and IT-related positions. These designations are required to distinguish and categorize the impact individuals having certain IT privileges could have on DoD functions and operations.

In today's environment, personnel in nearly every work situation use a computer to perform their assigned duties. In most of these situations, IT systems and resources are used as tools that enhance the incumbent's ability to accomplish their assignments. While these positions may require knowledge of various applications and skill in using available IT resources, the incumbents are not involved in developing, delivering, or supporting IT systems and services, or safeguarding sensitive data within such systems. Such IT users do not occupy IT positions and are not subject to the requirements of this Appendix.

The appendix also includes investigative, adjudicative and due process requirements associated with these positions. The requirements of this appendix, with the exception of Section 10, Adjudication, are to be applied to all IT and IT-related positions, whether occupied by DoD civilian employees, military personnel, consultants, contractor personnel or others affiliated with DoD (e.g., volunteers). Section 10 applies only to contractor personnel.

2. DEFINITIONS

For Official Use Only (FOUO)	DoD information that is not classified CONFIDENTIAL or higher IAW DoD 5200.1-R (reference (q) [revised January 1997]) and that may be withheld from public disclosure IAW DoD 5400.7-R, which implements the Freedom of Information Act (FOIA) (reference (ss)). FOUO information, though unclassified, nonetheless is sensitive and warrants protection from disclosure.
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Limited Privileged Access Privileged access with limited scope, e.g., an authority to change user access to data or system resources for a single information system (IS) or physically isolated network.

Non-privileged Access User level access, i.e., normal access given to a typical user. Generally, all access to system resources is controlled in a way that does not permit those controls/rules to be changed or bypassed.

Sensitive Information Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information in routine DoD payroll, finance, logistics, and personnel management systems. Examples of sensitive information include, but are not limited to, the following categories:

(1) **FOUO:** IAW DoD 5400.7-R, information that may be withheld from mandatory public disclosure under the Freedom of Information Act (FOIA) (reference (ss)). See definition above.
(2) **Unclassified Technical Data:** Data related to military or dual-use technology which is subject to approval, licenses or authorization under the Arms Export Control Act is withheld from public disclosure IAW DoD 5230.25.
(3) **Department of State Sensitive But Unclassified (SBU):** Information which originated from the Department of State (DoS) which has been determined to be SBU under appropriate DoS information security polices
(4) **Foreign Government Information:** Information which originated from a foreign government and which is not classified CONFIDENTIAL or higher but must be protected IAW DoD 5200.1-R (reference (q) [revised January 1997]).
(5) Privacy Data: Personal and private information (e.g., individual medical information, home address and telephone number, social security number) as defined in the Privacy Act of 1974 (reference (l)).

Privileged Access Authorized access that provides capability to alter the properties, behavior or control of the information system/network. It includes, but is not limited to, any of the following types of access:

(1) "Super user," "root," or equivalent access, such as access to the control functions of the information system/network, administration of user accounts, etc.
(2) Access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and other key information system/network equipment or software.
(3) Ability and authority to control and change program files, and other users' access to data.
(4) Direct access to operating system level functions (also called unmediated access) which would permit system controls to be bypassed or changed.
(5) Access and authority for installing, configuring, monitoring or troubleshooting the security monitoring functions of information systems/networks (e.g., network/system analyzers; intrusion detection software; firewalls) or in performance of cyber/network defense operations.

3. GENERAL GUIDANCE

3.1 DoDD 5200.28 (reference (zz)) specifies that information systems/networks shall be safeguarded through use of a mixture of administrative, procedural, physical, communications, emanations, computer, and personnel security measures, that together achieve the requisite level of security. As DoD becomes increasingly dependent upon information technology to execute the DoD mission, ensuring the trustworthiness of all personnel, including temporary, seasonal, and intermittent employees, contractors, and volunteers, in IT positions is critical.

3.2 The requirements of this appendix are intended to enhance the security of DoD IT systems and networks and to safeguard sensitive information. In those cases where sensitive information (e.g., Privacy Act data) is maintained in contractor owned and operated IT systems that have no interconnection (including data feeds) with DoD IT systems or networks, other safeguards (e.g., non-disclosure agreements, training) authorized in accordance with other applicable guidance may be used at the IT-III level in lieu of background investigations to mitigate the risks associated with the loss/misuse or unauthorized access to or modification of sensitive data.

3.3 Paragraph 5, below, will help to determine IT position categorization. Other scope and impact factors not specifically identified in paragraph 5 may be considered. Such factors may support changing the category of the position based on the agency's judgement as to the unique characteristics of the information system/network or the safeguards protecting the system/network.

3.4 Paragraph 5 also provides suggested category assignment by IT specialty. Other categorization schemes exist for IT positions (e.g., the Clinger-Cohen core competencies). This regulation uses Office of Personnel Management's (OPM's) GS-2200A, Information Technology Management series IT specialties because the information

and descriptions in the OPM IT classification standard can be easily recognized by both IT personnel and non-IT management who may have to make categorization determinations. Furthermore, the OPM standard, position titles, and associated information are descriptive and use language that can be easily related to position descriptions and personnel requirements.

3.5 Several factors must be considered to determine the category of an IT position. The most significant factors are: 1) the type of access (privileged or non-privileged), that signifies an incumbent's authorization to effect the operation of DoD information systems and networks, and 2) the potential adverse impact the incumbent could have on the Department's overall security posture or ability to execute its mission. Other factors are the IT specialty, the level of IT knowledge required for effective performance, and the opportunity to affect security and the intended operation or contents of the system/network.

3.6 Many IT positions involve a mixture of responsibilities and may cover multiple specialty titles. After analysis of a position's aggregated privilege, scope and level of independence, the position should be categorized at the highest level required by the specific duties, risks, and safeguards in place.

3.7 This policy applies to contractors and consultants in IT and IT-related positions and shall be implemented through incorporation in their contracts.

3.8 For cases in which the investigative requirements for an IT position exceed the investigative requirements for access to classified information/security clearance requirements, the higher requirement must be met. In such instances, an SF86 will be used.

3.9 Users of this appendix are also cautioned that other policies may levy additional requirements that must be met prior to assignment to a particular IT-related position. For example, each Designated Approving Authority (DAA), Information System Security Managers (ISSM), and Information System Security Officer (ISSO) must be a U.S. citizen; DAAs additionally must be U.S. Government personnel. Similarly, Verifying Officials (VO) and personnel appointed to operate Certificate Management Authority (CMA) equipment in support of DoD Public Key Infrastructure (PKI) must be U.S. citizens. It is the user's responsibility to be aware of additional requirements pertinent to the specific IT environment and to factor those requirements into this process at the appropriate places.

4. IT POSITION CATEGORIES

This paragraph provides broad guidance for categorizing IT and IT-related positions based on the level of information system/network access required to execute responsibilities of the position and on the potential for adverse impact on the DoD mission. DoD agencies that issue contracts requiring access to DoD IT resources/systems/network shall provide specific guidance to their contractors regarding the categorization of contractor IT positions and the investigative requirements of this regulation.

4.1 **IT-I Position** – Incumbent of this position has privileged access to networks and information systems, system security and network defense systems, or to system resources; duties are broad in scope and authority, and provide access to the U.S. Government, DoD, or Component mission critical systems. The potential exists for exceptionally serious adverse impact on U.S. Government, DoD, Component or private sector information and/or operations, with worldwide or government-wide effects. Incumbent may also be responsible for unsupervised funds disbursements or transfers or financial transactions totaling over $10M per year.

4.2 **IT-II Position** – Incumbent of this position has limited privileged access, but duties are of considerable importance to the DoD or DoD Component mission, and the incumbent is under the supervision of an individual in a higher trust position (IT-I). For example, individuals in these positions may have ability to impact a limited set of explicitly defined privileged functions, such as privileged access confined to large portions of an IS or to a local network physically isolated from other DoD or publicly accessible networks. The potential exists for moderate to serious adverse impact on DoD or Component information or operations. Incumbent may also be responsible for monitored/audited funds disbursements or transfers or financial transactions totaling less than $10M per year.

4.3 **IT-III Position** – Incumbent in this position has non-privileged access to one or more DoD information systems/applications. IT-III incumbents can receive, enter and/or modify information in an information system/application or database to which they are authorized access. Users have access only to that data/information and those applications/networks to which the incumbent is explicitly authorized or has need-to-know and cannot alter those or other users' authorizations. Positive security measures and configuration management ensure that the incumbent can assume only explicitly authorized roles and privileges. The potential exists for limited adverse impact on DoD, Component or unit information or operations. Incumbent may also be responsible for financial operations subject to routine supervision or approval, but has no funds disbursement or transfer capabilities.

5. TYPICAL CATEGORY ASSIGNMENT BY IT SPECIALTY

5.1 DoD components are responsible for categorization of each IT position at the highest level required by the specific duties, risks, and safeguards in place after analysis of the position's aggregated privileges, scope and levels of independence. Positions may be categorized at higher or lower levels as needed to account for ability to impact overall network/system security posture, intended

system behavior, or appropriate content. However, when level of privilege and other position characteristics appear to indicate differing levels of categorization, the higher categorization assignment should be used. Positions in all specialty areas that have greater degrees of management, training or administrative responsibility/duties than technical responsibilities for IT are generally less sensitive than IT positions requiring detailed technical insight or hands-on competency, or positions providing supervision/ oversight of technical positions at a lower categorization. DoD Components may take into consideration existing measures and practices for protecting sensitive information in their impact/risk assessment.

5.2 The following are typical category assignments for each IT specialty title defined in the OPM Position Classification Standard "Administrative Work in the Information Technology Group, GS-2200" (http://www.opm.gov/FEDCLASS/gs2200a.pdf). Other IT-related positions should be categorized based on the particular set of duties and responsibilities of the position and the scope, and level of privileges authorized. See also "IT Position Category Assignment Table" below.

a. Policy and Planning (PLCYPLN) – IT-III (IT-II if responsible for information security/ information assurance program or if individual also has privileged access)
b. Security (INFOSEC) – IT-I (IT-II if primarily policy, planning or awareness focused)
c. Systems Analysis (SYSANALYSIS) – IT-III (IT-II if responsible for information security/information assurance systems)
d. Applications Software (APPSW) – IT-I, -II, or –III depending on specifics of application (IT-I if responsible for information security/information assurance applications)
e. Operating Systems (OS) – IT-II (IT-I if incumbent acts independently, without oversight/review)
f. Network Services (NETWORK) – IT-I or IT-II (depending on the scope of network—as defined by criticality of or impact on Department or Federal government mission, geographic reach, and/or major or significant impact on other government agencies and/or the private sector—and level of privileges)
g. Data Management (DATAMGT) – IT-III (IT-II if responsible for safeguarding sensitive data/information)
h. Internet (INET) – IT-II (IT-I if privileged access to network functions)
i. Systems Administration (SYSADMIN) – IT-I (IT-II if stand-alone system or if ability to compromise limited to system/network operation)
j. Customer Support (CUSTSPT) – IT-III (IT-I if privileged access; or IT-II if ability to set/change user access privileges (scope and level sensitive))

5.3 Other activities or specialties that may have significant IT duties include the following:
a. Computer Clerk and Assistant (GS-335) or Computer Operation (GS-332) – typically IT-III, but may be higher if there is access to system/network control functions.

b. Telecommunications (GS-391) (e.g., computer network analysts; data communications) – use appropriate IT specialty in paragraph 5.2 above
c. Computer engineer (GS-0854) – generally hardware focused; typically IT-III, but specific categorization depends on function and application of the specific hardware/component (e.g., chip/board design may be IT-I), degree of supervision/review by higher authority, etc.
d. Computer Science (GS-1550) – categorization depends on specific duties/ responsibilities; use appropriate IT specialty in paragraph 5.2 above where possible.
e. Criminal Investigating (GS-1811) – Law enforcement activities associated with computer/network crime (e.g., forensic analysis; criminal investigation) – categorization depends upon required level of access (e.g., privileged/non-privileged).
f. Miscellaneous Management and Program Analysis (GS-343) and other scientists, subject matter experts, and professionals — depends upon required level of access (e.g., privileged/nonprivileged).
g. Technical editors and other subject matter experts who develop web pages, but whose primary expertise is not technical knowledge of Internet systems, services, and technologies – categorize under "Internet" IT specialty; if non-privileged access, may be assigned IT-III designation
h. Miscellaneous IT specialists (As required by specifics of new technology/ evolving specialty area) – use appropriate IT specialty in paragraph 5.2 above where possible.
i. Threat and vulnerability assessment (e.g., red-teams; penetration testing) – determined by the purpose and scope of the assessment objective and required level of access.
j. Certificate Management Authorities (CMA) to include Verifying Officials (VO) - typically IT-II, but may be higher if operating CMA equipment associated with Public Key Infrastructure operating above the DoD Class 4 assurance level.

IT Position Category Assignment Table

Categorization is based on assessment of the potential adverse impact (e.g., exceptionally serious, moderate to serious, or limited) a typical incumbent could have, given the stated combination of IT position characteristics.

IT Position Characteristics **IT Specialist (ITSPEC) Category***	***Privileged Access*** – Super User/Root Access to DoD IS ***Independence*** – Independent of routine supervision	***Limited Privileged Access*** – Privileged access with limited scope – Ability to set/change accesses or system resources on single IS or standalone network ***Independence*** – Subject to periodic/spot supervision/monitoring/audits by IT-I	***Nonprivileged Access*** – User level access to one or more DoD IS – No ability to set or change accesses or system resources ***Independence*** – Subject to routine review/supervision
Policy and Planning (PLCYPLN)	IT-II	IT-II	IT-III
Security (INFOSEC)	IT-I	IT-I	IT-II
Systems Analysis (SYSANALYSIS)	IT-II	IT-III	IT-III
Applications Software (APPSW)	IT-I	IT-II	IT-III
Operating Systems (OS)	IT-I	IT-II	IT-II
Network Services (NETWORK)	IT-I	IT-I	IT-II
Data Management (DATAMGT)	IT-II	IT-II	IT-III
Internet (INET)	IT-I	IT-II	IT-II
Systems Administration (SYSADMIN)	IT-I	IT-I	IT-II
Customer Support (CUSTSPT)	IT-I	IT-II	IT-III

Other *(Miscellaneous IT specialists, management, subject matter experts, etc.— categorization depends upon required level of access)*	IT-I	IT-II	IT-III

** (as defined by the OPM Position Classification Standard "Administrative Work in the Information Technology Group, GS-2200"* (http://www.opm.gov/FEDCLASS/gs2200a.pdf)*)*

6. ACCESS BY NON-U.S. CITIZENS

6.1 Every effort shall be made to ensure that non-U.S. citizens are not employed in IT positions. However, compelling reasons may exist to grant access to DoD IT resources in those circumstances where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed for a specific DOD requirement and for which a suitable U.S. citizen is not available.

6.2 Access to sensitive information by a non-U.S. citizen shall only be permitted IAW applicable disclosure policies (e.g. National Disclosure Policy 1, DoDD 5230.9, DoDD 5230.25) and U.S statutes (e.g., Arms Export Control Act). A non-U.S. citizen shall not be assigned to a DoD IT position requiring access to information which is not authorized to be disclosed.

6.3 Provided that information to which the incumbent will have access is authorized for foreign disclosure, non-U.S. citizens assigned into DoD IT positions are subject to the investigative requirements outlined in paragraph 7.

6.3.1 Non-U.S. citizens may hold/be authorized access to IT-II and IT-III positions when the conditions described in paragraphs 6.1 and 6.2 exist if the Designated Approving Authority (DAA) approves the assignment in writing. The written approval must be on file before requesting the required investigation. The required investigation must be completed and favorably adjudicated prior to authorizing IT-II and IT-III access to DoD systems/networks. Interim access is not authorized.

6.3.2 A non-U.S. citizen may be assigned to an IT-I position when the conditions described in paragraphs 6.1 and 6.2 exist and the Head of the DoD Component or Agency that owns the system/information approves the assignment in writing. The written approval must be on file before requesting the required investigation. The required investigation must be completed and favorably adjudicated prior to authorizing IT-I access to DoD systems/networks. Interim access is not authorized.

7. LEVEL OF BACKGROUND INVESTIGATION

The required investigations for all IT-I, IT-II and IT-III positions are outlined below.

Position Category	Civilian	Military	Contractor	Non-U.S. Citizen
IT-1	SSBI	SSBI	SSBI	SSBI, if approval granted
IT-II	NACIC	NACLC	NACLC	NACLC
IT-III	NACIC	NAC	NAC	NAC

Assignment (including assignments due to accretion of duties) of current DoD employees, military personnel, consultants and contractors to positions with different responsibilities or changed access privileges

requires verification of the appropriate investigative basis/authority for holding a position of that level of sensitivity.

8. REQUESTS FOR INVESTIGATION

8.1 All requests for investigations for IT positions that do not require access to classified information shall be initiated using the Questionnaire for Public Trust Positions, SF 85P with Supplemental Questionnaire and SF87/FD 258, Fingerprint Card. The form shall be completed only after a conditional offer of employment.

8.2 OPM Procedures

8.2.1 The SF85P and Supplemental Questionnaire (printed form with signed release(s)), FD258 fingerprint card, and Agency Use Block Information attachment (see page K-14) are to be mailed to: U.S. Office of Personnel Management (OPM), Federal Investigations Processing Center, P.O. Box 700, 1137 Branchton Road, Boyers, PA 16018-0700.

8.2.2 Each submitting office will need to establish a submitting office number (SON) with OPM. To obtain a SON, complete PIPS Form 12 (see page K-15) and fax it to OPM at (724) 794-2891. Your office must place this SON code on each request submitted to OPM.

8.2.3 When completing the Agency Use Block information, all requests must indicate one of the following central adjudication numbers, as appropriate, in Item L:

Army.....A334	DIA..... DD08
Navy.....NV00	WHS..... DD02
Air Force...AF00	OPM..... OM25 (contractors only)
NSA.....SP00	

8.2.4 When completing Item N, indicate the appropriate billing code.

8.3 For cases in which the investigative requirements for an IT position exceed the investigative requirements for access to classified information, the higher requirement must be met. In such instances, an SF86 will be used.

9. INTERIM ASSIGNMENT

9.1 Individuals, except non-U.S. citizens, to include temporary, intermittent and seasonal personnel, may be assigned to IT-I, IT-II, and IT-III positions on an interim basis prior to a favorable adjudication of the required personnel security investigation only after the conditions specified below have been met. Interim access is not authorized for non-U.S. citizens.

9.1.1 **IT-I**:

- Favorable completion of the NAC (current within 180 days)
- Initiation of an SSBI/favorable review of SF85P and Supplemental Questionnaire

9.1.2 **IT-II**:

- A favorable review of local personnel, base/military, medical, and other security records as appropriate
- Initiation of a NACIC (for civilians) or NACLC (for military and contractors), as appropriate/favorable review of SF85P and Supplemental Questionnaire

9.1.3 **IT-III**:

- A favorable review of local personnel, base/military, medical, and other security records as appropriate
- Initiation of a NACIC (for civilians) or NAC (for military and contractors), as appropriate/favorable review of SF85P and Supplemental Questionnaire

9.2 For DoD civilian and military personnel, the approval for interim assignment shall be made by the security manager at the requesting activity. For DoD contractor personnel, the approval shall be made by the government sponsor's security manager/official.

10. ADJUDICATION

10.1 The provisions of this section apply only to contractor personnel. Civilian employees, military personnel, consultants, volunteers, and seasonal, part-time and intermittent employees will be adjudicated by the appropriate DoD central adjudication facility.

10.2 All investigations conducted by OPM in accordance with this appendix will be adjudicated by OPM for a trustworthiness determination using the national adjudicative guidelines for access to classified information. If the adjudication is favorable, OPM will issue a letter of trustworthiness to the requesting activity.

10.3 If a favorable trustworthiness determination cannot be made, OPM will forward the case to the Defense Office of Hearings and Appeals (DOHA) in Columbus, OH, for further processing under DoDD 5220.6. A final unfavorable decision precludes assignment to an IT-I, II, or III position.

10.4 All OPM IT trustworthiness determinations of DoD contractor personnel will be entered into the OPM Security and Suitability Investigative Index (SII).

11. REINVESTIGATION

Individuals occupying an IT position shall be subject to a periodic reinvestigation according to prevailing policy.

12. PRIOR BACKGROUND INVESTIGATIONS

If an individual previously has been subject to background investigative and adjudicative requirements, depending on the age and scope of the investigation those requirements may not need to be duplicated for assignment to an IT position. Investigative criteria for DoD personnel and contractors/consultants who have had prior background investigations are outlined in the table below.

IT Position Category/Investigative Equivalency Table

DoD Civilian and Military Personnel, Contractors, and Consultants

If Position Category is:	***Individual has/had the following investigation:***	***And the age of the investigation is:***	***Then the investigation required is:***
IT-I	SSBI SSBI-PR	< 5 yrs	None
		> 5 yrs	SSBI-PR
	SBI BI LBI MBI NACLC ANACI NAC NACIC ENTNAC	Regardless of age of the investigation	SSBI
IT-II	SSBI SSBI-PR SBI BI LBI MBI NACLC ANACI NACIC	< 10 yrs	None
		> 10 yrs	NACLC
	ENTNAC NAC	Regardless of age of the investigation	NACLC (contractor, military) NACIC (civilian)
IT-III	SSBI SBI BI SSBI-PR LBI MBI ANACI NACLC NACIC ENTNAC NAC	< 15 yrs	None
		> 15 yrs	NAC (contractor, military) NACIC (civilian)

13. TRAINING AND AWARENESS REQUIREMENTS

DoD Components must ensure that individuals performing IT functions within the designated category receive the requisite information assurance, security awareness, and functional competency training. Understanding the threats, system vulnerabilities, and protective measures required to counter such threats are key features to a core information assurance awareness program at each IT position level.